

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [semantic-mediawiki.org](#) > 78.47.118.255

SSL Report: [semantic-mediawiki.org](#) (78.47.118.255)

Assessed on: Sat, 19 Dec 2015 15:03:19 UTC | **HIDDEN** | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating

A+

Certificate

Protocol Support


Key Exchange

Cipher Strength

020406080100


- Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).
- This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks.
- This server supports HTTP Strict Transport Security with long duration. Grade set to A+. [MORE INFO »](#)

Authentication



[Server Key and Certificate #1](#)

Subject	www.semantic-mediawiki.org Fingerprint SHA1: d6f75bd03d27fffd391a6130b48c8c413ad7930d Pin SHA256: yBzayWGngjmrFA3rEkKH9H5wLV9Nx7rsZo6v+ILYsWg=
Common names	www.semantic-mediawiki.org
Alternative names	www.semantic-mediawiki.org semantic-mediawiki.org
Prefix handling	Both (with and without WWW)
Valid from	Wed, 16 Dec 2015 05:43:28 UTC
Valid until	Fri, 16 Dec 2016 14:05:09 UTC (expires in 11 months and 26 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	StartCom Class 1 Primary Intermediate Server CA
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	Yes



[Additional Certificates \(if supplied\)](#)

Certificates provided	2 (3147 bytes)
Chain issues	None

#2

StartCom Class 1 Primary Intermediate Server CA

Subject	Fingerprint SHA1: 0ad38a30abc0f0b605b45c727a90819e7ff9daf4 Pin SHA256: kb6xLprt35abNnSn74my4Dkfy9arbk5zN5a60YzuqE=
Valid until	Fri, 14 Oct 2022 20:54:17 UTC (expires in 6 years and 9 months)
Key	RSA 2048 bits (e 65537)
Issuer	StartCom Certification Authority
Signature algorithm	SHA256withRSA



Certification Paths

Path #1: Trusted

1	Sent by server	www.semantic-mediawiki.org Fingerprint SHA1: d6f75bd03d27fffd391a6130b48c8c413ad7930d Pin SHA256: yBzayWGngjmrFA3rEkKH9H5wLV9Nx7rsZo6v+ILYsWg= RSA 2048 bits (e 65537) / SHA256withRSA
2	Sent by server	StartCom Class 1 Primary Intermediate Server CA Fingerprint SHA1: 0ad38a30abc0f0b605b45c727a90819e7ff9daf4 Pin SHA256: kb6xLprt35abNnSn74my4Dkfy9arbk5zN5a60YzuqE= RSA 2048 bits (e 65537) / SHA256withRSA
3	In trust store	StartCom Certification Authority Self-signed Fingerprint SHA1: 3e2bf7f2031b96f38ce6c4d8a85d3e2d58476a0f Pin SHA256: 5C8kvU039KouVrl52D0eZSGf4Onjo4Khs8tmyTIV3nU= RSA 4096 bits (e 65537) / SHA1withRSA Weak or insecure signature, but no impact on root certificate

Path #2: Trusted

1	Sent by server	www.semantic-mediawiki.org Fingerprint SHA1: d6f75bd03d27fffd391a6130b48c8c413ad7930d Pin SHA256: yBzayWGngjmrFA3rEkKH9H5wLV9Nx7rsZo6v+ILYsWg= RSA 2048 bits (e 65537) / SHA256withRSA
2	Sent by server	StartCom Class 1 Primary Intermediate Server CA Fingerprint SHA1: 0ad38a30abc0f0b605b45c727a90819e7ff9daf4 Pin SHA256: kb6xLprt35abNnSn74my4Dkfy9arbk5zN5a60YzuqE= RSA 2048 bits (e 65537) / SHA256withRSA
3	In trust store	StartCom Certification Authority Self-signed Fingerprint SHA1: a3f1333fe242bfcfc5d14e8f394298406810d1a0 Pin SHA256: 5C8kvU039KouVrl52D0eZSGf4Onjo4Khs8tmyTIV3nU= RSA 4096 bits (e 65537) / SHA256withRSA

Configuration



Protocols

TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No



Cipher Suites (SSL 3+ suites in server-preferred order; deprecated and SSL 2 suites at the end)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 2048 bits FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	DH 2048 bits FS	256

TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 2048 bits FS	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)	DH 2048 bits FS	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)	DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 2048 bits FS	128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a)	DH 2048 bits FS	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)	DH 2048 bits FS	128



Handshake Simulation

Android 2.3.7 No SNI ²	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DH 2048 FS
Android 4.0.4	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
Android 4.1.1	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
Android 4.2.2	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
Android 4.3	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
Android 4.4.2	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Android 5.0.0	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Baidu Jan 2015	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
BingPreview Jan 2015	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Chrome 47 / OS X R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 31.3.0 ESR / Win 7	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 42 / OS X R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Googlebot Feb 2015	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
IE 6 / XP No FS ¹ No SNI ²	Protocol or cipher suite mismatch		
IE 7 / Vista	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
IE 8 / XP No FS ¹ No SNI ²	Protocol or cipher suite mismatch		
IE 8-10 / Win 7 R	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
IE 11 / Win 7 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
IE 11 / Win 8.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
IE 10 / Win Phone 8.0	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
IE 11 / Win Phone 8.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS
IE 11 / Win Phone 8.1 Update R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
IE 11 / Win 10 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Edge 13 / Win 10 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Edge 13 / Win Phone 10 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Java 6u45 No SNI ²	Client does not support DH parameters > 1024 bits		
	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DH 2048
Java 7u25	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 FS
Java 8u31	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
OpenSSL 0.9.8y	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DH 2048 FS
OpenSSL 1.0.1l R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
OpenSSL 1.0.2 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Safari 5.1.9 / OS X 10.6.8	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
Safari 6 / iOS 6.0.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
Safari 6.0.4 / OS X 10.8.4 R	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
Safari 7 / iOS 7.1 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
Safari 7 / OS X 10.9 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
Safari 8 / iOS 8.4 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
Safari 8 / OS X 10.10 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
Safari 9 / iOS 9 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Apple ATS 9 / iOS 9 R	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS

[Yahoo Slurp Jan 2015](#)

TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS

[YandexBot Jan 2015](#)

TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS

- (1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.
- (2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.
- (3) Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.
- (R) Denotes a reference browser or client, with which we expect better effective security.
- (All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).



Protocol Details

Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0xc014
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	Yes
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
Forward Secrecy	Yes (with most browsers) ROBUST (more info)
Application-Layer Protocol Negotiation (ALPN)	No
Next Protocol Negotiation (NPN)	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	Yes
Strict Transport Security (HSTS)	Yes max-age=31536000
HSTS Preloading	Chrome Edge Firefox IE Tor semantic-mediawiki.org
Public Key Pinning (HPKP)	No
Public Key Pinning Report-Only	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No
DH public server param (Ys) reuse	No
SSL 2 handshake compatibility	Yes



Miscellaneous

Test date	Sat, 19 Dec 2015 15:01:05 UTC
Test duration	134.135 seconds
HTTP status code	200
HTTP server signature	Apache/2.4.12 (Ubuntu)
Server hostname	static.255.118.47.78.clients.your-server.de

